12 FAM 600
INFORMATION SECURITY TECHNOLOGY

12 FAM 610
ORGANIZATION AND PURPOSE OF COMPUTER SECURITY (COMPUSEC)

(TL:DS-69; 06-22-2000)

12 FAM 611 PURPOSE AND SCOPE

(TL:DS-69; 06-22-2000)

a. It is the policy of the Department of State to establish and maintain an effective *automated information system (AIS)* security program *for* the protection of *Department AISs*. 1 FAM assigns responsibility for the development and oversight of the Department's *AIS* security program. This 12 FAM subchapter assigns implementational responsibility for the Department's *AIS* security program. These *AIS* security policies comply with and implement Federal statutes, policies, and directives regarding the protection of information and *AIS* equipment for the Department and the foreign affairs community.

b. The Bureau of Diplomatic Security has developed worldwide *policies* for *all* Department classified and unclassified *AISs, regardless of hardware platform.* These *policies* are designed to protect information pertaining to national security and foreign relations, as well as information defined as sensitive by the Department of State. (See 12 FAM 000.)

c. These *policies* were developed in consultation with the Overseas Security Policy Board (OSPB) and the Department's regional and functional bureaus.

12 FAM 612 APPLICABILITY

12 FAM 612.1 Domestic

(TL:DS-69; 06-22-2000)

a. All Department of State *AISs* processing classified or unclassified information in the United States are subject to the requirements of this chapter.

b. Other U.S. Government agencies with stand-alone *AISs* processing classified information in Department of State facilities or agencies processing classified or sensitive unclassified information on *AISs* or equipment connected to DOS *AISs* are subject to the *requirements of this chapter.*

12 FAM 612.2 Abroad

(TL:DS-69; 06-22-2000)

a. All Department of State *AISs* processing classified or unclassified information at Foreign Service posts are subject to the *requirements of this chapter.*

b. The following criteria constitute the basis for determining the applicability of all Department of State *AIS* security policies to the *AISs* of agencies under the authority of a chief of mission or principal officer. Information concerning intelligence sources and methods is handled or processed under Director of Central Intelligence guidelines.

c. The applicability of *AIS* security policy for unclassified *AISs* is based on connectivity to Department of State *AISs.* All foreign affairs agencies with *AISs* or peripherals connected to Department *AISs* are required to comply with the requirements of this chapter.

d. Foreign affairs agencies with stand-alone *AISs* processing unclassified sensitive information are responsible for providing adequate *AIS* security, as mandated by Federal requirements. Individual agencies at post are responsible for identifying those *AISs that* contain unclassified sensitive information.

e. At the request of a chief of mission or principal officer, DS/CIS/IST will evaluate the *AIS* security of another agency's stand-alone *AISs* to ensure compliance with U.S. national standards.

f. All foreign affairs agencies processing unclassified information in controlled access areas (CAAs) at critical technical threat posts are required to comply with *the requirements of this chapter.*

g. All Department of State *AIS* security policies for classified *AISs* are applicable to all agencies operating under the authority of a chief of mission or principal officer.

h. Foreign affairs agencies may provide their own software to their post representatives upon the following conditions:

(1) There is no connection between the other agency's *AIS* and those of the Department of State;

(2) The software is not used on any Department of State *AIS*; and

(3) The agency provides *proof of accreditation to the Department of State Designated Approving Authority (DAA) and* certifies that the software has been properly tested, protected, and controlled, including shipment to post by classified pouch.

12 FAM 613 RESPONSIBILITIES

(TL:DS-69; 06-22-2000)

The Bureau of Diplomatic Security is responsible for the administration and management of the *AIS* security program for the Department of State, domestically and abroad, and for other Federal agencies under the authority of a chief of mission or principal officer as defined in this section. The following are responsible for the implementation of policy.

12 FAM 613.1 Officer in Charge, Engineering Services Center or Office

(TL:DS-69; 06-22-2000)

The officer in charge of an engineering services center or office (ESC or ESO) is responsible for providing regional technical engineering support for post installation of physical and technical security safeguards in areas containing *AISs*. In addition, the OIC provides technical support to DS/CIS/IST during evaluations abroad and performs the site survey for the installation of classified *AIS* equipment.

12 FAM 613.2 Director, Regional Information Management Center (RIMC)

(TL:DS-69; 06-22-2000)

The director of a regional information management center (RIMC) is responsible for providing communications maintenance and repair support to constituent posts. The director also provides technical support to DS/CIS/IST during evaluations *abroad* and performs the site survey for the installation of classified equipment. In addition, the director is responsible for providing *AIS* training and ensuring that *AIS* security requirements established by DS/CIS/IST are incorporated into training materials and responses to requests for guidance received from constituent posts.

12 FAM 613.3 Administrative Officer and Executive Director

(TL:DS-69; 06-22-2000)

The administrative officer or executive director is responsible for overall management of *AISs* at their post or bureau. This individual ensures that an information systems security officer (ISSO) is formally appointed for each *AIS* and coordinates implementation of Department *AIS* security policies. The administrative officer or executive director may delegate these responsibilities as necessary.

12 FAM 613.4 Regional and Post Security Officers

(TL:DS-69; 06-22-2000)

The regional or post security officer (RSO or PSO) is responsible for security, including *AIS* security as established by DS/CIS/IST. The security officer is responsible for ensuring that appropriate personnel security practices are implemented, that adequate physical security measures are applied, that *AIS* security is included in security training programs, and that contingency plans for *AISs* are coordinated with emergency action plans (12 FAH-1, *Emergency Planning Handbook*). The security officer, assisted by the ISSO, also investigates suspected security incidents involving *AISs*.

12 FAM 613.5 Security Engineering Officer and Seabee

(TL:DS-69; 06-22-2000)

The security engineering officer (SEO) or assigned Seabee installs and maintains physical and technical security systems and equipment, advises the RSO or PSO on physical and technical security issues, and reviews existing or proposed security for *AIS* installations for compliance with relevant Department *AIS security policies.*

12 FAM 613.6 Marine Security Guards and DS Uniformed Protective Officers

(TL:DS-69; 06-22-2000)

Marine security guards (MSGs) or DS uniformed protective officers perform security inspections of Department facilities worldwide to ensure that users of *AISs* comply with *AIS* security policies mandated by DS/CIS/IST and issue security violations for noncompliance.

12 FAM 613.7 Regional Computer Security Officer (RCSO)

(TL:DS-69; 06-22-2000)

The regional computer security officer (RCSO) provides guidance and assistance on a regional basis to posts worldwide. The RCSO reports to the Director of DS/CIS/IST on all matters relating to *AIS* security. The individual implements criteria for access controls, storage, transmission, and destruction of data maintained by *AISs* at posts, and monitors post compliance with those criteria. The RCSO conducts on-site *AIS* security evaluations of classified and unclassified *nonmainframe AISs* and prepares formal reports detailing findings and recommendations. The RCSO supplements standard *AIS* security training materials with specific information tailored to post requirements and processing environments, and supports contingency planning efforts. Where there is no RCSO assigned, posts should refer questions to DS/CIS/IST.

12 FAM 613.8 Mainframe Security Program Manager

(TL:DS-69; 06-22-2000)

The Mainframe Security Program Manager, (IRM/OPS/ITI/SI), is responsible for implementing and managing the Department's AIS security program for mainframe AISs. The Mainframe Security Program Manager is responsible for providing coordination and guidance to all mainframe ISSOs on the implementation of DS AIS security policies for classified and unclassified mainframe AISs. The Mainframe Security Program Manager is responsible for issuing procedural or operational documentation in the form of SI documents to mainframe ISSOs within subject offices. He or she must be a U.S. citizen Department of State employee.

12 FAM 613.9 Corporate Information Systems Security Officer (CISSO)

(TL:DS-69; 06-22-2000)

The corporate information systems security officer (CISSO) is responsible for managing and implementing the Department's AIS security program. He or she is responsible for providing coordination and guidance to all ISSOs. The CISSO works with the network ISSO and system manager to allow individual AISs to link into the Department's enterprise AIS infrastructure. The CISSO works with DS on the certification and accreditation of individual AISs. He or she must be a Department of State employee and U.S. citizen.

12 FAM 613.10 Information Systems Security Officer (ISSO)

12 FAM 613.10-1 Client Server Information Systems Security Officer (ISSO)

(TL:DS-69; 06-22-2000)

The client server information systems security officer (ISSO) implements the *Department's AIS* security *program on all classified and unclassified nonmainframe AISs*. *He or she* advises the security officer on *AIS* security issues and works closely with the system manager, *the corporate ISSO, and* the information programs officer (IPO). *The client server ISSO also works with DS, the system manager and the corporate ISSO to certify and accredit individual AISs and to allow for AIS linkage into the Department's enterprise AIS infrastructure.* The ISSO must be a U.S. citizen Department of State employee. However, at the discretion of the administrative officer, another security officer, such as the RSO or PSO, can also act as the ISSO.

12 FAM 613.10-2 Mainframe Applications Information Systems Security Officer (ISSO)

(TL:DS-69; 06-22-2000)

The mainframe information systems security officer (ISSO) implements the Department's AIS security program on all classified and unclassified mainframe AISs. He or she advises the program manager on AIS security issues and works closely with the Mainframe Systems Security Program staff (IRM/OPS/ITI/SI) to implement DS AIS security policies and IRM AIS security procedures. The mainframe applications ISSO must be a Department of State employee and a U.S. citizen.

12 FAM 613.11 Information Management Officer (IMO)

(TL:DS-69; 06-22-2000)

The information management officer (IMO) is responsible for the overall management of contingency planning and for the overall management of information management programs and personnel, including the planning, development, and evaluation of *AIS* hardware and software, the administration of local area networks and databases, and oversight of significant resources. This individual is responsible for ensuring that DS *AIS* security *policies* are implemented at their facility. In those foreign locations where no cleared U.S. citizen exists, the information program officer (IPO) is responsible for overall *AIS* management.

12 FAM 613.12 Information Program Officer (IPO)

(TL:DS-69; 06-22-2000)

The information program officer (IPO) implements DS *AIS* security policies for communications. The IPO is also responsible for the installation, maintenance, and operation of encryption equipment used in conjunction with *AISs* and the control of cryptographic material.

12 FAM 613.13 COMSEC Custodian

(TL:DS-69; 06-22-2000)

The COMSEC custodian is responsible for the receipt, transfer, accountability, safeguarding, and destruction of COMSEC material issued to a COMSEC account. In coordination with DS/CIS/IST, the IMO or IPO ensures facility compliance with national and Department COMSEC policy.

12 FAM 613.14 Regional Information Systems Officer (RISO)

(TL:DS-69; 06-22-2000)

The regional information systems officer (RISO) is responsible for providing ISSOs and system managers with advice and support to ensure the proper operation and management of all *AISs* served by the designated regional information management center (RIMC). The RISO also ensures that all *AIS* security controls established by DS/CIS/IST are correctly implemented on served by the RIMC.

12 FAM 613.15 Data Center Manager

(TL:DS-69; 06-22-2000)

The data center manager has the overall responsibility and accountability for ensuring that all DS AIS security policies are implemented for all classified and unclassified, abroad and domestic, mainframe AISs under his or her authority. For the large IRM operations centers throughout the Department, this would be the responsibility of the ISSO to encompass all the systems in the IRM operations center.

12 FAM 613.16 System Manager

(TL:DS-69; 06-22-2000)

The system manager is responsible for proper operation and management of *classified and unclassified nonmainframe AISs*. The system manager implements security controls on the *AISs* as established by DS/CIS/IST and provides advice and support to the ISSO and security officer on *AIS* security issues. The system manager supervises the system staff in implementing DS *AIS* security *policies*.

12 FAM 613.17 Application Programmer

(TL:DS-69; 06-22-2000)

The application programmer is responsible for following the security *policies* for life-cycle management issued by DS/CIS/IST when developing or performing maintenance on a new or existing application.

12 FAM 613.18 Mainframe Systems Programmer

(TL:DS-69; 06-22-2000)

The mainframe systems programmer is responsible for the installation of all mainframe computer software, including maintenance and upgrade releases. He or she is the direct link between the ACF2 security staff (IRM/OPS/ITI/SI) and the mainframe computer staff (IRM/OPS/SIO/MFS).

12 FAM 613.19 Personnel Officer

(TL:DS-69; 06-22-2000)

The personnel officer is responsible for ensuring that a statement assigning responsibility for *AIS* security is included in position descriptions for *AIS*

systems staff. In addition, the personnel officer will ensure that the personnel checkout process includes the *AIS* systems staff.

12 FAM 613.20 General Services Officer (GSO)

(TL:DS-69; 06-22-2000)

The general services officer (GSO), in conjunction with the senior information management officer and the system manager, contributes to the process that ensures that physical facilities for *AISs* are constructed, modified, and maintained in accordance with *policies* issued by responsible organizations, such as the Office of Foreign Building Operations or the Bureau of Diplomatic Security.

12 FAM 613.21 Program Managers

(TL:DS-69; 06-22-2000)

Program managers are responsible for determining, in a coordinated effort with the system manager, which users have a verified need to access their applications, as mandated by DS/CIS/IST standards. The program managers are also responsible for informing the ISSO of any security incidents related to the application or the users of the application.

12 FAM 613.22 System Staff

(TL:DS-69; 06-22-2000)

System staff members are responsible for following appropriate *AIS* security *policies*, maintaining required logs and records as assigned, and monitoring the system for abnormal operation.

12 FAM 613.23 User Supervisors

(TL:DS-69; 06-22-2000)

User supervisors ensure that users adhere *AIS* security *policies* and authorize access to new users based upon their functional requirements.

12 FAM 613.24 AIS Users

(TL:DS-69; 06-22-2000)

AIS users must abide by DS *AIS* security *policies* and report any *AIS* or

application irregularities or suspected security violations to appropriate personnel.

12 FAM 613.25 Application Developers

(TL:DS-69; 06-22-2000)

Application developers ensure that appropriate safeguards and *AIS* security *policies* are incorporated into all new *AIS* applications, as well as significant modifications to existing *AIS* applications. This includes any applications that they develop or maintain, including design, review, and system acceptance testing.

12 FAM 613.26 Technical Services and Safeguards Officer (TSSO)

(TL:DS-69; 06-22-2000)

The technical services and safeguards officer (TSSO) is responsible for ensuring that, at posts where plain text processing equipment (PTPE) is used, all PTPE physical, technical, and procedural security programs are implemented.

12 FAM 613.27 Communications Electronic Officer

(TL:DS-69; 06-22-2000)

The communications electronic officer services all classified *AISs* and TEMPEST microcomputers (classified and unclassified) at Foreign Service posts.

12 FAM 613.28 Cleared American Technician (CAT)

(TL:DS-69; 06-22-2000)

The cleared American technician (CAT) services all classified *AISs* and TEMPEST microcomputers (classified and unclassified) at designated Foreign Service posts under the direction of the information management officer, the system manager, or the communications program officer.

12 FAM 614 AUTHORITIES

(TL:DS-51; 04-12-1996)

a. Omnibus Diplomatic Security and Antiterrorism Act of 1986, 22 U.S.C. 4804 (2)(B) and (5).

b. Computer Security Act of 1987, 40 U.S.C. 759.

c. Privacy Act of 1974, 5 U.S.C. 552a(e)(10).

d. The Immigration and Nationality Act, 8 U.S.C. 1202, Section 222(f).

e. Federal Manager's Financial Integrity Act, 31 U.S.C. 1352.

f. Computer Fraud and Abuse Act of 1986, 18 U.S.C. 1030.

g. Executive Order No. 12958 entitled, "Classified National Security Information."

h. Executive Order 10421 entitled, "Providing for the Physical Security of Facilities Important to the National Defense."

i. "National Policy for Safeguarding and Control of Communications Security (COMSEC) Material," NCSC-1.

j. "National Policy on Use of Crypto-Material by Activities Operating in High-Risk Environments," NCSC-5.

k. "National Policy on Secure Voice Communications," NCSC-8.

l. National Telecommunications and Information System Security Policy 3 (NTISSP 3), "National Policy for Granting Access to U.S. Classified Cryptographic Information."

m. National Telecommunications and Information System Security Policy 200 (NTISSP 200), "National Policy on Controlled Access Protection."

n. National Telecommunications and Information System Security Policy 300 (NTISSP 300), "National Policy on Control of Compromising Emanations."

o. National Telecommunications and Information System Security Directive 500 (NTISSD 500), "National Directive on Telecommunications and Automated Information Systems Security (TAISS) Education, Training, and Awareness."

p. National Telecommunications and Information System Security Directive 600 (NTISSD 600), "National Directive on Communications Security (COMSEC) Monitoring."

q. "National Policy on Telecommunications and Automated Information Systems Security."

r. Director of Central Intelligence Directive 1/16 (DCID 1/16).

s. Office of Management and Budget Circular A-130 (OMB A-130).

t. Office of Management and Budget Circular A-123 (OMB A-123).

u. Federal Personnel Manual.

v. The National Security Telecommunications and Information Systems Security Committee (NSTISSC) instructions and advisory memoranda.

12 FAM 615 DEPARTMENT RESPONSIBILITIES

12 FAM 615.1 Assistant Secretary, Bureau of Diplomatic Security (DS)

(TL:DS-69; 06-22-2000)

See 1 FAM for DS responsibilities. The responsibilities for the Assistant Secretary include, but are not limited to: acting as the certification authority for the Department of State; developing information technology security policy for the Department; conducting reviews of system security plans; maintaining the regional computer security officer program; conducting the computer awareness training program; implementing and monitoring the Department's Intrusion Detection Program; maintaining the Computer Incident Response Team; maintaining the computer forensics program; performing computer and communication security evaluations; conducting and issuing formal risk and vulnerability assessments and coordinating information technology security policy with other U.S. Government agencies that are part of the Overseas Security Policy Board. The Assistant Secretary is jointly responsible with the Chief Information Officer (CIO) for the development and implementation of a comprehensive, technically current, and cost-effective AIS security program for the Department. The AIS security program will include classified and unclassified, domestic and overseas, mainframe and nonmainframe AISs. The program will also comply with established National Security Directives.

12 FAM 615.1-1 Deputy Assistant Secretary, Countermeasures and Information Security (DS/CIS)

(TL:DS-69; 06-22-2000)

See 1 FAM for DS/CIS responsibilities. These include assisting the Assistant Secretary in formulating *AIS* security policy and programs, and *providing* management oversight to the:

(1) Office of Information Security Technology;

(2) Office of Domestic Operations;

(3) Office of Physical Security Programs; and

(4) Office of the Diplomatic Courier Service.

12 FAM 615.1-2 Director, Office of Information Security Technology (DS/CIS/IST)

(TL:DS-69; 06-22-2000)

See 1 FAM for DS/CIS/IST responsibilities.

12 FAM 615.1-3 Director, Office of Physical Security Programs (DS/CIS/PSP)

(TL:DS-69; 06-22-2000)

See 1 FAM for DS/CIS/PSP responsibilities. These include establishing policies for the procurement, secure transit, and secure storage of materials, to include *AISs*, destined for the CAA.

12 FAM 615.1-4 Director, Office of Domestic Operations (DS/CIS/DO)

(TL:DS-69; 06-22-2000)

See 1 FAM for DS/CIS/DO responsibilities. These include establishing the physical security requirements for domestic facilities and ensuring that new domestic facilities or renovations to existing domestic facilities comply with approved Department design standards.

12 FAM 615.1-5 Chief, Technology Operations Division (DS/ST/STO)

(TL:DS-69; 06-22-2000)

See 1 FAM for DS/ST/STO responsibilities.

12 FAM 615.1-6 Chief, Countermeasures Program Division (DS/ST/CMP)

(TL:DS-69; 06-22-2000)

See 1 FAM for DS/IST/CMP responsibilities.

12 FAM 615.1-7 Chief, Office of Investigations and Counterintelligence, Personnel Security/Suitability Division (DS/ICI/PSS)

(TL:DS-69; 06-22-2000)

See 1 FAM for DS/ICI/PSS responsibilities. These include issuing cryptographic clearances.

12 FAM 615.1-8 Director, Office of Professional Development, Training Center (DS/PLD/TC)

(TL:DS-69; 06-22-2000)

See 1 FAM for DS/PLD/TC responsibilities. These include the central administration of the Department's *AIS* security training and awareness program. DS/CIS/IST is responsible for providing technical expertise and resources to support *AIS* security training.

12 FAM 615.1-9 Director, Office of the Diplomatic Courier Service (DS/CIS/DC)

(TL:DS-69; 06-22-2000)

See 1 FAM for DS/CIS/DC responsibilities.

12 FAM 615.2 Director, Foreign Service Institute (M/FSI)

(TL:DS-69; 06-22-2000)

See 1 FAM for M/FSI responsibilities. *These include* integrating *AIS* security training into the FSI training curriculum based upon guidance provided by DS/CIS/IST.

12 FAM 615.3 Chief Information Officer, Bureau of

Information Resources Management (IRM)

(TL:DS-69; 06-22-2000)

a. See 1 FAM for the CIO, Bureau of Information Resources Management's responsibilities. These include directing and administering the Department's AIS security program for classified and unclassified, mainframe and nonmainframe AISs abroad and domestic.

b. Serving as the principal adviser to the Secretary of State on the development, implementation, and as necessary, the revision of policies, plans, and programs for information resources management. The CIO has been given broad authority from the Secretary to coordinate the modernization of Department AISs. This includes setting Department-wide information technology standards and oversight of Department information resources policies, plans and programs.

c. When necessary, CIO will be the mediator for all disputes between Department entities regarding mainframe operational, procedural or implementation issues.

12 FAM 615.3-1 Deputy Chief Information Officer for Operations (IRM/OPS)

(TL:DS-69; 06-22-2000)

See 1 FAM for IRM/OPS responsibilities. These include developing and implementing operational procedures for the Department's AIS security program for classified and unclassified, mainframe and nonmainframe AISs abroad and domestic.

12 FAM 615.3-2 Director, Information Technology Infrastructure (IRM/OPS/ITI)

(TL:DS-69; 06-22-2000)

See 1 FAM for IRM/OPS/ITI responsibilities. *These include* the implementation procedures for *AIS* security policies developed by DS/CIS/IST for cryptographic, communications, *AISs*. IRM/OPS/ITI manages the Department of State's cryptographic account and inventory as well as the cryptographic clearance program for use and access to post communication centers.

12 FAM 615.3-3 Chief, Systems Integrity Division(IRM/OPS/ITI/SI)

(TL:DS-69; 06-22-2000)

See 1 FAM for IRM/OPS/ITI/SI responsibilities. These include reviewing and evaluating operational procedures for the Department's AIS security program for classified and unclassified, mainframe and nonmainframe AISs abroad and domestic.

12 FAM 615.3-4 Director, Systems and Integration (IRM/OPS/SIO)

(TL:DS-69; 06-22-2000)

See 1 FAM for IRM/OPS/SIO responsibilities. *These include coordinating* the development of new *AISs* and major revisions to existing *AISs* with DS/CIS/IST to ensure that security is incorporated into *AISs* at their inception.

12 FAM 615.4 Assistant Secretary, Bureau of Administration (A)

(TL:DS-69; 06-22-2000)

See 1 FAM for A responsibilities.

12 FAM 615.4-1 Deputy Assistant Secretary, Foreign Building Operations (A/FBO)

(TL:DS-69; 06-22-2000)

See 1 FAM for A/FBO responsibilities. These include ensuring that DS physical *AIS* security requirements are incorporated into the design and construction of new office buildings and major renovations of existing facilities. In addition, the DAS ensures that Department *AIS* facilities are included in the fire and safety inspection program. The DAS, in coordination with DS/CIS, also ensures that these facilities comply with all national physical safety and security requirements.

12 FAM 615.4-2 Deputy Assistant Secretary, Office of Operations (A/OPR)

(TL:DS-69; 06-22-2000)

See 1 FAM for A/OPR responsibilities. These include, based upon guidance from DS/CIS, *ensuring* the inclusion of appropriate security elements in the

review of contracts for information systems and services. In addition, the Director institutes appropriate procedures to ensure compliance with the security aspect of the Federal procurement policies.

12 FAM 615.5 Assistant Secretary, Bureau of Intelligence and Research (INR)

(TL:DS-69; 06-22-2000)

See 1 FAM for INR responsibilities. These include acting as the responsible accreditation authority for *AIS*s processing or transmitting sensitive compartmented information (SCI) and grants or denies accreditation based upon a security recommendation of the Director of DS/CIS/IST. The Assistant Secretary for INR has delegated this authority to the Assistant Secretary for Diplomatic Security for collateral systems; however, only the Assistant Secretary for INR may accredit an *AIS* or network for operation in the compartmented mode as specified in DCID 1/16.

12 FAM 615.6 The Inspector General (OIG)

(TL:DS-69; 06-22-2000)

See 1 FAM for OIG responsibilities. These include performing audits and inspections to monitor compliance with *AIS* policies and ensure compliance with DS *AIS* security evaluation recommendations. The Inspector General also investigates suspected *AIS*-related fraud, theft, or misuse of Department *AIS* assets with technical assistance from DS.

12 FAM 615.7 Chief Financial Officer, Bureau of Finance and Management Policy (FMP)

(TL:DS-69; 06-22-2000)

See 1 FAM for FMP responsibilities. These include *providing* guidance to DS to ensure that the *AIS* security program is consistent with the goals and objectives of the Department's Internal Controls Program.

12 FAM 615.8 Chief of Mission, Principal Officer, and Bureau Assistant Secretary

(TL:DS-69; 06-22-2000)

The chief of mission (COM), principal officer (PO), or bureau Assistant

Secretary, ensures that Department *AIS* security policies are implemented and maintained on all Department *AISs* operating under his or her authority. This individual may delegate the authority necessary to implement security *policies* to appropriate personnel.

12 FAM 616 THROUGH 619 UNASSIGNED